WHAT IS CLAIMED IS:

1. A method performed by a custodian to share a secret S among n secret owners, the method comprising the steps of:

choosing two large primes P and Q;

computing a product $N = PQ$;

computing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers q_1 through q_n that are relatively prime to M;

determining a number d such that a product of q_1 through q_n and d mod M equals one;

computing S^d;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^d and one of the numbers q_1 through q_n; and

deleting the secret S, P, Q, M, q_1 through q_n, and d.

2. A method as in claim 1, the method further comprising the steps of:

receiving a first of the n secret owner pieces from one of the n secret owners; and

computing and storing $S' = S^{dq} \bmod N$, where q represents the one of the numbers q_1 through q_n contained in the first of the n secret owner pieces.

3. A method as in claim 2, the method further comprising the steps of:

receiving a second of the n secret owner pieces from another one of the n secret owners;

computing $S'^q \bmod N$, where q represents the one of the numbers q_1 through q_n contained in the second of the n secret owner pieces; and replacing S' with $S'^q \bmod N$.

4. A method as in claim 3, further comprising the step of:

each time another of the secret owner pieces is received from another one of the n secret owners;

computing S'^{q} mod N, where q represents the one of the numbers q_1 through q_n contained in another of the n secret owner pieces; and replacing S' with S'^{q} mod N.

5. A method performed by a custodian to share a secret S among n secret owners, the method comprising the steps of:

choosing two large primes P and Q;

computing a product $N = PQ$;

computing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n+1 random numbers q_1 through q_n and d' that are relatively prime to M;

determining a number d such that a product of q_1 through q_n, d', and d mod M equals one;

computing S^d;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^d and one of the numbers q_1 through q_n; and

deleting the secret S, P, Q, M, q_1 through q_n, and d.

6. A method as in claim 5, the method further comprising the steps of:

receiving a first of the n secret owner pieces from one of the n secret owners; and

computing and storing $S' = S^{dq}$ mod N, where q represents the one of the numbers q_1 through q_n contained in the first of the n secret owner pieces.

7. A method as in claim 6, the method further comprising the steps of:

receiving a second of the n secret owner pieces from another one of the n secret owners;

computing S'^{q} mod N, where q represents the one of the numbers q_1 through q_n contained in the second of the n secret owner pieces; and

replacing S' with S'^{q} mod N.

8. A method as in claim 7, further comprising the step of:

each time another of the secret owner pieces is received from another one of the n secret owners;

computing $S'^{q} \bmod N$, where q represents the one of the numbers q_1 through q_n contained in the another of the n secret owner pieces; and

replacing S' with $S'^{q} \bmod N$.

9. A method as in claim 8, further comprising the steps of:

after all n secret owner pieces has been received;

computing $S'^{d'} \bmod N$; and

replacing S' with $S'^{d'} \bmod N$.

10. A method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q, such that PQ is greater than S;

computing and storing a product $N = PQ$;

computing and storing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers e_1 through e_n that are relatively prime to N;

choosing another random number e that is relatively prime to N;

choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \le i \le n$;

choosing another number d such that $ed \bmod M$ is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$;

deleting P, Q, and M;

computing S^e;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^e and one of the numbers e_1 through e_n; and

deleting the secret S and e_1 through e_n, e, d_1 through d_n, and d.

11. A method as in claim 10, the method further comprising the steps of:

receiving a first of the n secret owner pieces from one of the n secret owners; and

computing and storing $S' = S^{ef} \bmod N$, where f represents the one of the numbers e_1 through e_n contained in the first of the n secret owner pieces.

12. A method as in claim 11, the method further comprising the steps of:

receiving a second of the n secret owner pieces from another one of the n secret owners;

computing $S'^q \bmod N$, where q represents the one of the numbers e_1 through e_n contained in the second of the n secret owner pieces; and replacing S' with $S'^q \bmod N$.

13. A method as in claim 12, further comprising the step of:

each time another of the secret owner pieces is received from another one of the n secret owners;

computing $S'^q \bmod N$, where q represents the one of the numbers e_1 through e_n contained in the another of the n secret owner pieces; and replacing S' with $S'^q \bmod N$.

14. A method as in claim 13, further comprising the steps of:

after k secret owner pieces have been received,

retrieving from the database a value c from among the $\binom{n}{k}$ values, wherein the value c corresponds to the k secret owner pieces that were received by the custodian;

computing $S'^c \bmod N$; and

replacing S' with $S'^c \bmod N$.

15. A method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q, such that PQ is greater than S;

computing and storing a product $N = PQ$;

computing and storing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers e_1 through e_n that are relatively prime to N;

choosing random numbers e and e' that are relatively prime to N;

choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \le i \le n$;

choosing numbers d and d' such that $ed \bmod M$ is equal to one and such that $e'd' \bmod M$ is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$;

deleting P, Q, and M;

computing $S^{ee'}$;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes $S^{ee'}$ and one of the numbers e_1 through e_n; and

deleting the secret S and e_1 through e_n, e, d_1 through d_n, and d.

16. A method as in claim 15, the method further comprising the steps of:

receiving a first of the n secret owner pieces from one of the n secret owners; and

computing and storing $S' = S^{ee'f} \bmod N$, where f represents the one of the numbers e_1 through e_n contained in the first of the n secret owner pieces.

17. A method as in claim 16, the method further comprising the steps of:

receiving a second of the n secret owner pieces from another one of the n secret owners;

computing $S'^{q} \bmod N$, where q represents the one of the numbers e_1 through e_n contained in the second of the n secret owner pieces; and replacing S' with $S'^{q} \bmod N$.

18. A method as in claim 17, further comprising the step of:

each time another of the secret owner pieces is received from another one of the n secret owners;

computing $S'^{q} \bmod N$, where q represents the one of the numbers e_1 through e_n contained in the another of the n secret owner pieces; and replacing S' with $S'^{q} \bmod N$.

19. A method as in claim 18, further comprising the steps of:

after k secret owner pieces have been received,

retrieving from the database a value c from among the $\binom{n}{k}$ values, wherein the value c corresponds to the k secret owner pieces that were received by the custodian; computing $S'^{c} \bmod N$;

replacing S' with $S'^{c} \bmod N$;

computing $S'^{d'} \bmod N$; and

replacing S' with $S'^{d'} \bmod N$.

20. A method performed by a custodian to share a secret among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

encrypting the secret so as to generate an encrypted secret;

deleting the secret; and

performing a forward k out of n secret sharing algorithm on the encrypted secret so as to generate n secret owner pieces.

21. A method as in claim 20, further comprising the step of:

distributing the n secret owner pieces to the n secret owners.

22. A method as in claim 21, further comprising the step of:

receiving k secret owner pieces from k secret owners.

23. A method as in claim 22, further comprising the step of:

performing a reverse k out of n secret sharing algorithm on the k secret owner pieces so as to recreate the encrypted secret.

24. A method as in claim 23, further comprising the step of:

decrypting the encrypted secret so as to recreate the secret.

25. A method as in claim 20, wherein the step of performing a forward k out of n secret sharing algorithm includes the steps of:

dividing the encrypted secret into k pieces; and

performing n polynomial evaluations at n points of a degree-k polynomial using the k pieces of the encrypted secret as polynomial coefficients;

wherein each of the k secret owner pieces includes a result of one of the n polynomial evaluations and a corresponding one of the n points.

26. A method as in claim 25, further comprising the steps of:

distributing the n secret owner pieces to the n secret owners;

receiving k secret owner pieces from k secret owners; and

performing a reverse k out of n secret sharing algorithm on the k secret owner pieces so as to recreate the encrypted secret; wherein the step of performing a reverse k out of n secret sharing algorithm includes the steps of generating a system of k linear equations and solving the system of k linear equations for the k pieces of the encrypted secret.

27. A method as in claim 26, further comprising the step of:

assembling the k pieces of the encrypted secret so as to recreate the encrypted secret; and

decrypting the encrypted secret so as to recreate the secret.

28. A computer readable storage medium having embodied thereon computer readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners, the method comprising the steps of:

choosing two large primes P and Q;

computing a product $N = PQ$;

computing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers q_1 through q_n that are relatively prime to M;

determining a number d such that a product of q_1 through q_n and d mod M equals one;

computing S^d;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^d and one of the numbers q_1 through q_n; and

deleting the secret S, P, Q, M, q_1 through q_n, and d.

29. A computer readable storage medium having embodied thereon computer readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners, the method comprising the steps of:

choosing two large primes P and Q;

computing a product $N = PQ$;

computing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n+1 random numbers q_1 through q_n and d' that are relatively prime to M;

determining a number d such that a product of q_1 through q_n, d', and d mod M equals one;

computing S^d;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^d and one of the numbers q_1 through q_n; and

deleting the secret S, P, Q, M, q_1 through q_n, and d.

30. A computer readable storage medium having embodied thereon computer readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q, such that PQ is greater than S;

computing and storing a product $N = PQ$;

computing and storing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers e_1 through e_n that are relatively prime to N;

choosing another random number e that is relatively prime to N;

choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \le i \le n$;

choosing another number d such that $ed \bmod M$ is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$;

deleting P, Q, and M;

computing S^e;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^e and one of the numbers e_1 through e_n; and

deleting the secret S and e_1 through e_n, e, d_1 through d_n, and d.

31. A computer readable storage medium having embodied thereon computer readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q, such that PQ is greater than S;

computing and storing a product $N = PQ$;

computing and storing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers e_1 through e_n that are relatively prime to N;

choosing random numbers e and e' that are relatively prime to N;

choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \le i \le n$;

choosing numbers d and d' such that $ed \bmod M$ is equal to one and such that $e'd' \bmod M$ is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$;

deleting P, Q, and M;

computing $S^{ee'}$;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes $S^{ee'}$ and one of the numbers e_1 through e_n; and

deleting the secret S and e_1 through e_n, e, d_1 through d_n, and d.

32. A computer readable storage medium having embodied thereon computer readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

encrypting the secret so as to generate an encrypted secret;

deleting the secret; and

performing a forward k out of n secret sharing algorithm on the encrypted secret so as to generate n secret owner pieces.

33. A computer comprising a processor and a computer readable storage medium coupled to the processor having embodied thereon processor readable program code suitable for programming the computer to perform a method performed by a custodian to share a secret S among n secret owners, the method comprising the steps of:

choosing two large primes P and Q;

computing a product $N = PQ$;

computing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers q_1 through q_n that are relatively prime to M;

determining a number d such that a product of q_1 through q_n and d mod M equals one;

computing S^d;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^d and one of the numbers q_1 through q_n; and

deleting the secret S, P, Q, M, q_1 through q_n, and d.

34. A computer comprising a processor and a computer readable storage medium coupled to the processor having embodied thereon processor readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners, the method comprising the steps of:

choosing two large primes P and Q;

computing a product $N = PQ$;

computing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n+1 random numbers q_1 through q_n and d' that are relatively prime to M;

determining a number d such that a product of q_1 through q_n, d', and d mod M equals one;

computing S^d;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^d and one of the numbers q_1 through q_n; and

deleting the secret S, P, Q, M, q_1 through q_n, and d.

35. A computer comprising a processor and a computer readable storage medium coupled to the processor having embodied thereon processor readable program code suitable for programming a computer to perform a method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q, such that PQ is greater than S;

computing and storing a product $N = PQ$;

computing and storing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers e_1 through e_n that are relatively prime to N;

choosing another random number e that is relatively prime to N;

choosing n numbers d_1 through d_n such that $e_i d_i$ mod M equals one for $1 \le i \le n$;

choosing another number d such that ed mod M is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$;

deleting P, Q, and M;

computing S^e;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes S^e and one of the numbers e_1 through e_n; and

deleting the secret S and e_1 through e_n, e, d_1 through d_n, and d.

36. A computer comprising a processor and a computer readable storage medium coupled to the processor having embodied thereon processor readable program code suitable for programming the computer to perform a method performed by a custodian to share a secret S among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

choosing two large primes P and Q, such that PQ is greater than S;

computing and storing a product $N = PQ$;

computing and storing a product $M = (P\text{-}1)(Q\text{-}1)$;

choosing n random numbers e_1 through e_n that are relatively prime to N;

choosing random numbers e and e' that are relatively prime to N;

choosing n numbers d_1 through d_n such that $e_i d_i \bmod M$ equals one for $1 \le i \le n$;

choosing numbers d and d' such that $ed \bmod M$ is equal to one and such that $e'd' \bmod M$ is equal to one;

generating and storing a database of $\binom{n}{k}$ values, where each value is the product of d and a unique k of the d_i numbers for $1 \le i \le n$;

deleting P, Q, and M;

computing $S^{ee'}$;

distributing n secret owner pieces to each of the n secret owners, wherein each of the secret owner pieces includes $S^{ee'}$ and one of the numbers e_1 through e_n; and

deleting the secret S and e_1 through e_n, e, d_1 through d_n, and d.

37. A computer comprising a processor and a computer readable storage medium coupled to the processor having embodied thereon processor readable program code suitable for programming the computer to perform a method performed by a custodian to share a secret among n secret owners such that any k of the n secret owners may reconstruct the secret, the method comprising the steps of:

encrypting the secret so as to generate an encrypted secret;

deleting the secret; and

performing a forward k out of n secret sharing algorithm on the encrypted secret so as to generate n secret owner pieces.